REMARKS

The Office Action mailed April 1, 2009 has been carefully considered. Claims 49-58 are pending. Claims 49 and 54 are amended and claim 58 is newly added. No new matter has been added.

The 35 U.S.C. § 103 Rejection

Claims 49-57 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Martinek et al. (US 2003/0130032 A1), referred to as Martinek, in view of Arnold (EPO 0661675 A2).

Martinek describes a pass-through live validation system and method. The method is described using Figures 3 and 4, shown below.

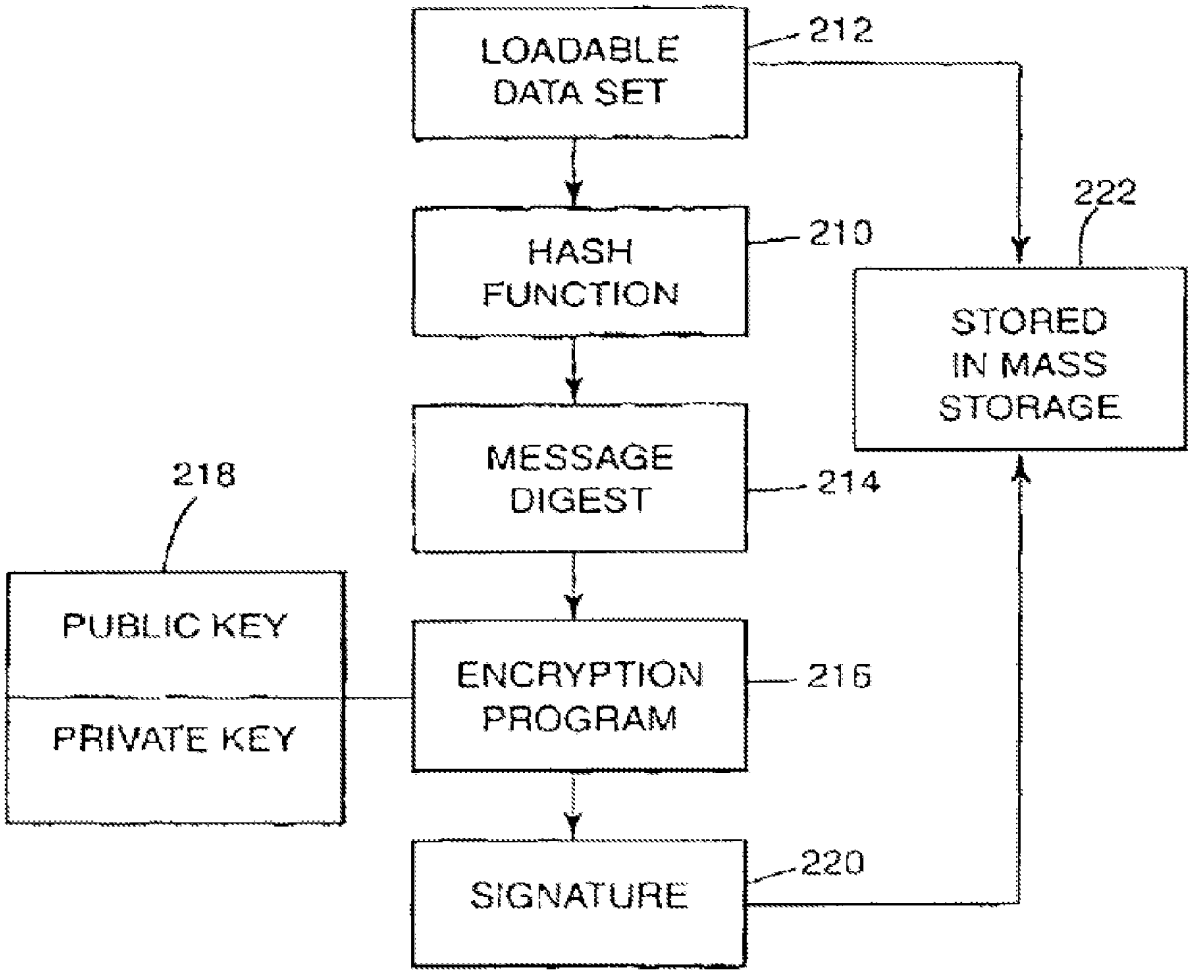

Fig. 3

The system includes a shared object code. The shared object code, as well as other data may be verified "by first preparing a signature from data, as shown in FIG. 3. The signature may be prepared by first hashing 210 the data set 212 to create a message digest 214. *The message digest is encrypted via an encryption program that is stored on ROM utilizing a private/public key algorithm 218, forming a unique signature 220*" (paragraph 79) (*Emphasis added*).

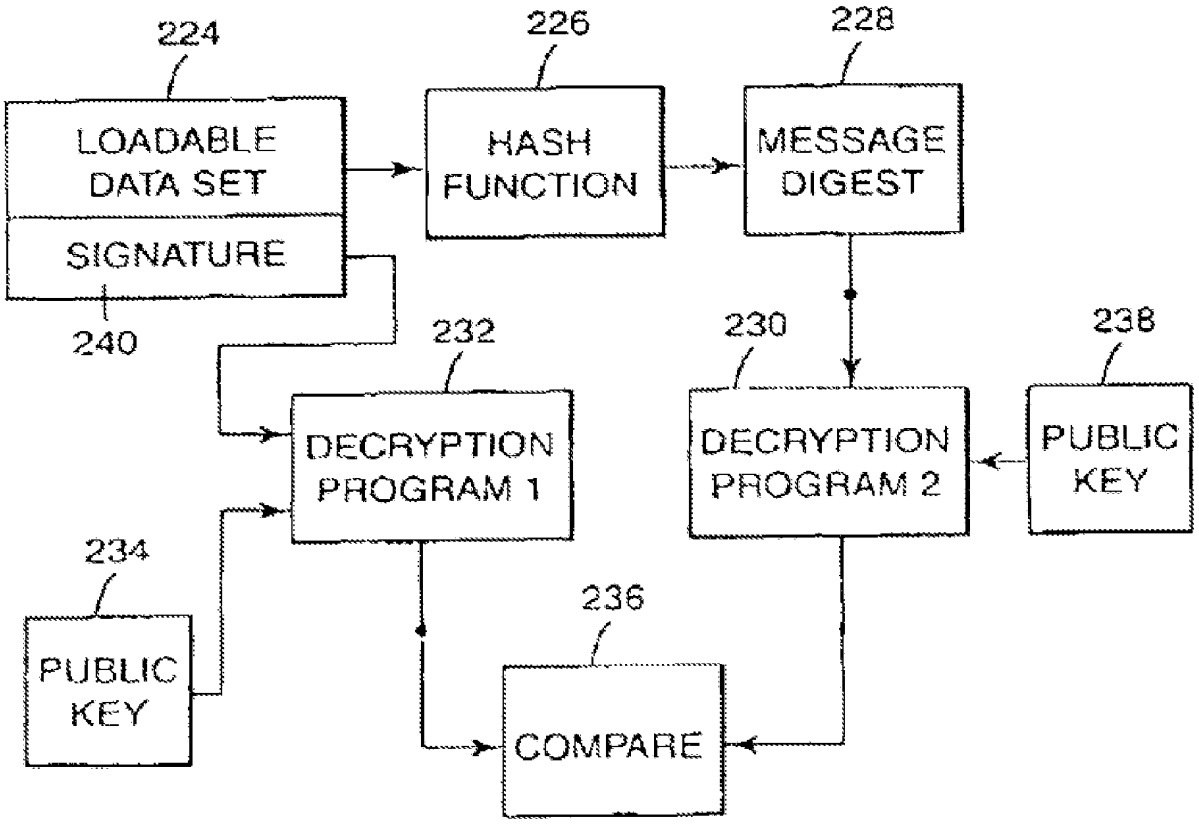

Fig. 4

"*The message digest 228 (as shown in FIG. 4) created from hashing the shared object is preferably encrypted, as part of the higher level verification processes*. A public key 238 is used to decrypt the message digest utilizing a first decryption program. The signature 240 stored in flash memory is decrypted using a second decryption program via a public key 234 and the values are compared 236" (paragraph 81) (*Emphasis added*). "In some embodiments using digital signatures, the digital signature is that of a regulatory agency ***or*** other organization responsible for ensuring the integrity of data in computerized wagering game systems. For example, the Nevada Gaming Regulations Commission may apply a signature to

data used in such gaming systems, ensuring that they have approved the signed data" (paragraph 83) (*Emphasis added*). "In other embodiments, the digital signature is that of the game code manufacturer or designer, and ensures that the game code has not been altered from its original state since signing" (paragraph 83).

Moreover, Arnold describes an access control system and method. The method is described with respect to Figures 1, 3 and 4, reproduced below. Figure 1 shows a user's card (21) and a supervisor's card (21).

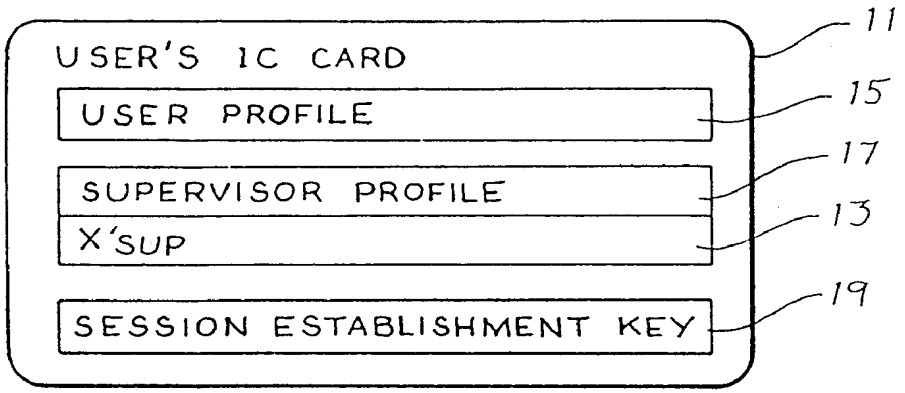

Fig. 1.

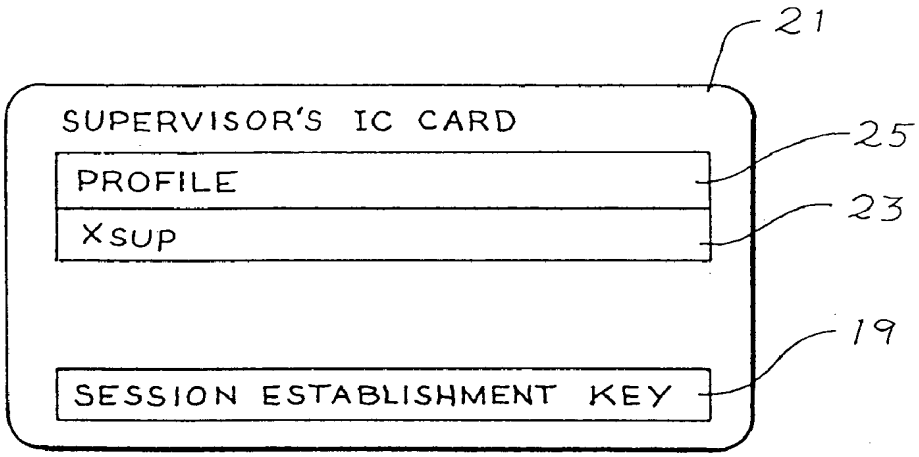

Fig. 2.

"The session establishment key 19 is an encryption key that is used by all devices in the system to establish sessions and a session key for each session between any two devices in the system. *The session establishment key in the supervisors card is the same as the session establishment key in the users card.* Likewise X'sup and Xsup are the same or related values. The encryption keys and the authorization values such as Xsup are not exposed outside of a

secure environment of an IC card or a card reader. *For this reason, they need not be changed or updated during the life of the card*" (col. 5, lines 31-42) (*Emphasis added*).

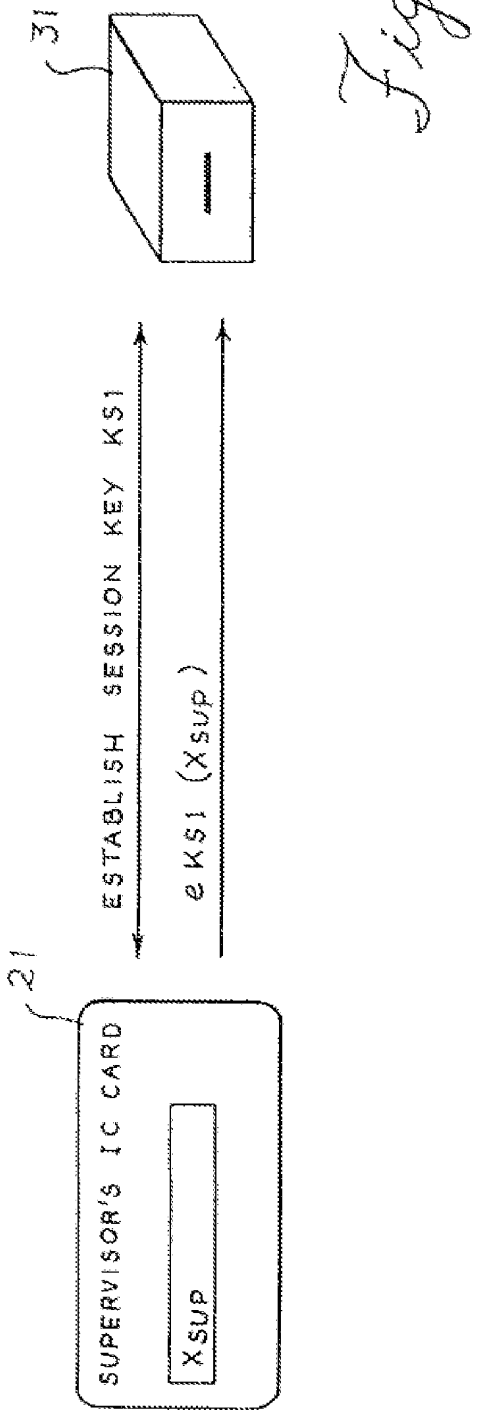

Fig. 3.

"Figure 3 shows the supervisor's card 21 and the card reader 31 and depicts the information flow necessary to establish a secure communication session and to transfer the value Xsup to the card reader 31" (col. 5, lines 44-47). "After the session key has been established, the IC card 21 *encrypts* the value Xsup under the session key KS1 which is depicted in the legend eKS1(Xsup) and is then sent to the reader 31 where it is decrypted and stored in a secure area for later use by the users card as the trial authorization value" (col. 5, lines 53-58).

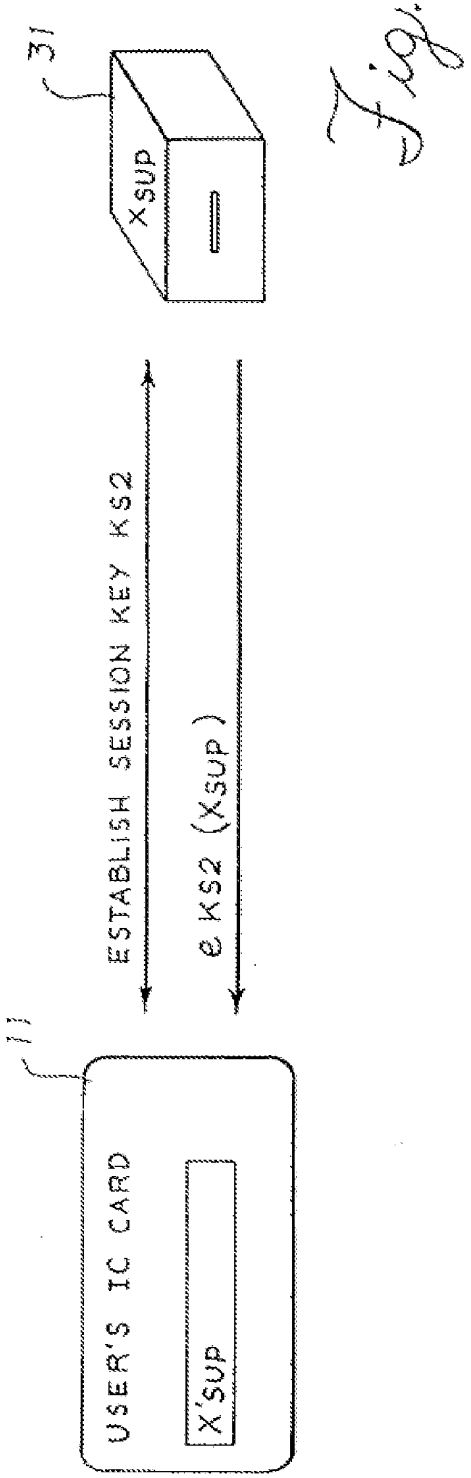

Fig. 4.

"Figure 4 shows the user's card 11 and the card reader 31 and depicts the information flow necessary to establish a secure communication session and to transfer the value Xsup

from the card reader 31. The session key is established in the same way as was done with the supervisors card but of course results in a new key value KS2. After the session key KS2 has been established, the card reader 31 *encrypts* the value Xsup under the session key KS2 which encryption is depicted in the legend eKS2(Xsup) and this encrypted value of Xsup is then sent to the user's card 11. At the user's card 11 it is decrypted and used as a trial authorization value for comparison" with a test authorization value X'sup stored in the user's card 11 (col. 6, lines 4-18) (*Emphasis added*).

Applicant respectfully submits that neither Martinek nor Arnold, considered alone or in combination, describe or suggest a gaming apparatus as recited in claim 49. For example, neither Martinek nor Arnold, considered alone or in combination, describe or suggest that "said controller being programmed to ***determine whether said first decrypted gaming data decrypted by using the encryption key of said first gaming organization is identical to said second decrypted gaming data decrypted by using the encryption key of said second gaming organization***" as recited in claim 49. Rather, Martinek describes **using a public key 238 to decrypt a message digest** and **using a second public key 234 to decrypt a signature 240** stored in flash memory, and comparing the decrypted values. Martinek further describes that Nevada Gaming Regulations Commission may **apply** a signature to data used in gaming systems and that in other embodiments, the digital signature is that of the game code manufacturer or designer.

However, Martinek does not describe or suggest that one encryption key is that of a first gaming organization and another encryption key is that of a second gaming organization. Further, the Examiner agrees that Martinek lacks "first encrypting gaming data with a first key from a first gaming organization and a second key from a second organization and decrypting the gaming data with the first and second keys from the first and second gaming organizations" (Office Action, page 4).

The Examiner further describes in the Office Action that "[t]he examiner believes that first encrypting gaming data with a first key from a first gaming organization and a second key from a second organization and decrypting the gaming data with the first and second keys from the first and second gaming organizations is obvious in light of Arnold" (Office Action, pages 4-5). The Examiner further explains on page 5 of the Office Action that:

'675 in Figs. 3, 4, and 5 shows a data set being encrypted with separate keys from separate entities (a user and a supervisor, analogous to a game developer and a Gaming Commission, respectively, of '032). Fig. 3, 5:44-6:3 of '675 describes a data set Xsup being encrypted with a supervisor's session key KS1. Fig. 4, 6:4-19 of '675 describes the same data set with a user's session key KS2. Fig. 5, 6:20-7:20 of '675 describes the computation of the decryption value using the supervisor's session key KS1 to recover Xsup and the computation of the decryption value using the user's session key KS2 to recover Xsup. If the two recovered values of Xsup are the same, the desired activity is allowed to continue (steps 65, 69, 71, Fig. 1).

Applicants respectfully disagree with the statements on page 5 of the Office Action. Specifically, Applicants respectfully submit that the description of the session keys in Arnold does not describe or suggest an encryption key of the first gaming organization that is different than a second organization having an encryption key. For example, Arnold describes that "*[t]he session establishment key in the supervisors card is the* ***same*** *as the session establishment key in the users card*" and that "*they need not be changed or updated during the life of the card*" (*Emphasis added*). This description in Arnold teaches away from the recitation regarding the "***first gaming data decrypted by using the encryption key of said first gaming organization***" and "***second decrypted gaming data decrypted by using the encryption key of said second gaming organization***". Gaming data is decrypted using the encryption key of the first gaming organization that is *different* than the second gaming organization that uses an encryption key to decrypt gaming data (*Emphasis added*). There is no mention or suggestion of this difference in Arnold. Rather, Arnold, to the contrary, describes that the same session key is used in both the user's and supervisor's card.

Further, Arnold has lesser security than that described in claim 49 because Arnold uses the same session key and claim 49 describes two encryption keys from two different gaming organizations. If a hacker gains access to the session key in Arnold, all communications under any session established using the session key may be accessible.

Hence, contrary to the statements made in the Office Action, Arnold does not describe or suggest an encryption key of the first gaming organization used to decrypt gaming data and an encryption key of a second gaming organization used to decrypt gaming data. Thus,

for at least the reasons set forth above, claim 49 is patentable over Martinek in view of Arnold.

Moreover, as an example, for at least the same reasons set forth above, neither Martinek nor Arnold, considered alone or in combination, describe or suggest "***determining whether said first decrypted gaming data decrypted by using the encryption key of said first gaming organization is identical to said second decrypted gaming data decrypted by using the encryption key of said second gaming organization***" as recited in claim 54. Hence, for at least the reasons set forth above, Applicants respectfully submit that claim 54 is patentable over Martinek in view of Arnold.

The various dependent claims are respectfully submitted to be patentable over the art of record for at least the same reasons as set forth above with respect to their associated independent claims. Furthermore, these dependent claims recite additional features that when considered in the context of the claimed invention, further patentably distinguish the art of record. Accordingly, for at least the reasons set forth above, claims 50-53 and 55-57 are patentable over Martinek in view of Arnold.

The Section 101 Rejection

Claims 54-57 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicant has amended claim 54. Hence, for at least the reasons set forth above, Applicant respectfully submits that claim 54 and its corresponding dependent claims are directed to statutory subject matter.

New claim 58

Claim 58 depends from independent claim 1, which is patentable over the cited art for at least the reasons set forth above. Accordingly, claim 58 is also patentable over the cited art.

Conclusion

Applicant hereby petitions for a one-month extension of time. It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited and Applicant respectfully requests that a timely Notice of Allowance be issued in this case. If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

Respectfully submitted,

/ David P. Olynick /
David P. Olynick
Reg. No. 48,615

Weaver Austin Villeneuve & Sampson LLP
P.O.Box 70250
Oakland, CA 94612-0250